Tema 4. Hacking ético

4.1 Introducción

En el mundo digital de la actualidad, las empresas comienzan a tener dificultades para proteger la información confidencial propia o de clientes, al mismo tiempo que buscan mantener una presencia importante en el negocio de las tecnologías de la información.

Una alternativa para alcanzar un nivel aceptable de protección de sus activos más importantes son las pruebas de penetración, un campo de la seguridad informática que ha crecido mucho últimamente y que permite a *hackers* éticos realizar evaluaciones de seguridad con la responsabilidad y honestidad siempre en mente.

Como último preludio a la realización concreta de nuestro proyecto, a continuación explicamos a detalle los conceptos en los que se basa el mismo, las pruebas de penetración, sus diferentes variantes y los pasos a seguir para llevarla a cabo de manera exitosa.

4.2 Definición

El *hacking* ético o pruebas de penetración "*es la práctica que una entidad confiable realiza para intentar comprometer la red de computadoras de una organización, con el propósito de evaluar su seguridad*". [111] Mediante la simulación de un ataque en vivo, los administradores pueden ser testigos del daño potencial que un atacante puede provocar al ganar acceso, destruir datos o dañar los valores de la compañía.

Las pruebas de penetración pueden ser de tres tipos:

- Pruebas de caja negra. No se tiene conocimiento alguno de la red que se probará. Se puede, por ejemplo, contar con una dirección web o IP e intentar ganar acceso a la misma como si se fuera un atacante externo.

- Pruebas de caja blanca. Se tiene un conocimiento total de la red interna. Puede contarse con diagramas de la red, listas de aplicaciones y de sistemas operativos, etc. A pesar de que no es una simulación realista de un ataque externo, es el más exacto en relación con el "peor escenario", aquel en el que el atacante también cuenta con total conocimiento de la red objetivo.

- Pruebas de caja gris. Se simula ser un empleado. Se tiene una cuenta de acceso estándar a la red interna, por tanto, es una prueba acerca de las amenazas que un empleado dentro de la compañía puede generar. [112]

[111] Andrew Whitaker, Daniel Newman, *Penetration testing and network defense*, Estados Unidos, Cisco Press, 2006, p. 5.
[112] *Idem*, p. 6.

4.3 Pasos a seguir

Antes de realizar una prueba de penetración hay algunas cosas que deben definirse, entre ellas, el ámbito en la que ésta se llevará a cabo. Algunos de los factores a considerar para definir correctamente dicho ámbito son los siguientes:

- Definir los horarios en los que la prueba se llevará a cabo (durante o después de las horas de trabajo).
- Definir si las denegaciones de servicio serán permitidas.
- Definir si troyanos y *backdoors* pueden ser instalados en los sistemas.
- Definir si podrá intentarse atacar los sitios web.
- Definir si las bitácoras podrán ser borradas.
- Definir si el tipo de prueba será de caja negra, blanca o gris.
- Determinar si los administradores están conscientes de que las pruebas se llevan a cabo. No es recomendable que estén informados porque es probable que busquen endurecer las medidas de seguridad, lo que provocará que los resultados obtenidos no muestren lo que normalmente pasaría dentro de la red en un ataque real.
- Determinar qué sistemas serán los objetivos de evaluación.
- Definir si se permitirá el empleo de la ingeniería social.
- Definir si se permitirá la obtención y remoción de información de los sistemas evaluados.
- Determinar mediante qué medios será distribuido el reporte de la prueba y a quién. [113]

Una vez que se ha estructurado el ámbito de la prueba se puede comenzar a realizarla. De manera general, ésta puede dividirse en las siguientes cinco etapas:

- Reconocimiento. En esta fase se reúne la mayor cantidad de información posible acerca del objetivo. Este reconocimiento puede ser activo, en el que se utilizan diversas herramientas para la obtención de la información deseada, o pasivo, en el que se utiliza información que está disponible públicamente para descubrir información acerca de las tecnologías que posee la compañía.
- Escaneo. En esta fase se busca determinar qué servicios y qué sistemas operativos corren en el sistema objetivo. Se realiza de manera general un

[113] *Idem*, pp.6-8.

escaneo de puertos que además de ayudar a recabar la información antes mencionada, nos pueden permitir identificar vulnerabilidades para ganar acceso al sistema posteriormente.

- Ganar acceso. Una vez realizado el escaneo de debilidades en la red, se procede a explotar tales fallas.

- Mantener acceso. Cuando se realiza con éxito la penetración en el sistema, generalmente se busca mantener el acceso al mismo para futuros ataques. Esto se logra mediante la instalación de *backdoors*.

- Cubrir rastros. La última fase de la prueba es la eliminación de evidencias. Muchos ataques se realizan sin ser detectados, por lo que es conveniente evaluar cuáles de ellos pueden ser exitosos al cubrir los rastros dejados. [114]

4.4 Informe de observaciones

Una prueba de penetración es inservible si no se tiene algo tangible para dar al cliente. Un informe de observaciones debe incluir los resultados de las pruebas y si es el caso, deben documentarse las recomendaciones para asegurar sistemas de alto riesgo.

El informe debe contener las siguientes secciones:

- Resumen ejecutivo. Es una descripción general corta de la prueba, escrito para ejecutivos clave que quieren saber cómo afectan los resultados a su compañía y que probablemente no le darán mucha importancia a los detalles técnicos. Incluye además, un caso de negocio detallando el impacto de los resultados y los costos asociados a la reparación de las vulnerabilidades descubiertas.

- Ámbito del proyecto. Debe incluir el rango de direcciones IP probadas y factores como si se utilizó la ingeniería social, si se probaron redes públicas o privadas, si se utilizaron troyanos o *backdoors*, por mencionar algunos. Debe incluir además, un estimado del número de *exploits* utilizados y el tipo de cada uno de ellos.

- Análisis de resultados. Esta la parte esencial del informe. La extensión de esta sección puede variar dependiendo del ámbito y los detalles de la prueba. Debe utilizarse una plantilla que incluya lo siguiente:

  i. Dirección IP y dominio del equipo probado.

  ii. Puertos *TCP* y *UDP* abiertos.

  iii. Descripción de los servicios.

[114] *Idem*, pp. 35-37.

iv. Pruebas realizadas.

v. Análisis de vulnerabilidades.

- Resumen. El resumen ejecutivo al inicio del informe está dirigido hacia aquellos que toman las decisiones clave; el resumen final está dirigido hacia el personal técnico. Debe contener una lista de recomendaciones técnicas para el cliente.

- Apéndice. Finalmente, el informe debe incluir un apéndice con las siguientes secciones:

  i. Información de contacto.

  ii. Impresiones de pantalla.

  iii. Registro de salida.

Las impresiones de pantalla y registros de salida son especialmente importantes. Se debe documentar todo lo que se hace durante la prueba para demostrar al cliente el trabajo realizado. [115]

[115] *Ídem*, pp. 40-45.